

United States District Court
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

FRISCO MEDICAL CENTER, L.L.P.	§	
d/b/a BAYLOR MEDICAL CENTER	§	
AT FRISCO	§	
	§	
V.	§	CASE NO. 4:12-CV-37/4:15cv105
	§	Judge Mazzant
CYNTHIA A. BLEDSOE and	§	
MICHAEL R. BLEDSOE	§	

MEMORANDUM OPINION

Pending before the Court is Plaintiff’s Motion for Summary Judgment (Dkt. #190). Having considered the motion, and the lack of response thereto, the Court finds that the motion should be granted.

BACKGROUND

Plaintiff Frisco Medical Center, L.L.P. d/b/a Baylor Medical Center at Frisco (“Baylor Frisco”) is a hospital that provides a broad range of surgical procedures and health care for residents of North Texas. As part of its delivery of quality health care, as a health care facility, Baylor Frisco is subject to the Health Insurance Portability and Accountability Act (“HIPAA”), and must enact safeguards to ensure that protected health information pertaining to individuals or patient-identifying information that is protected from disclosure by HIPAA is not disclosed or disseminated. Baylor Frisco also has a peer review committee that conducts peer review activities, which are privileged and confidential. Baylor Frisco has developed, compiled, and maintained a substantial amount of non-public, patient health information, as well as confidential and proprietary information and trade secrets, including, without limitation, information relating to its delivery of patient care, marketing, safety practices, and strategic planning.

Baylor Frisco actively seeks to maintain the confidentiality of such information by requiring employees to agree to and execute confidentiality agreements, pursuant to which its employees agree to maintain the confidentiality of Baylor Frisco's confidential information and to refrain from disseminating such information.

Defendant Cynthia A. Bledsoe ("Ms. Bledsoe") is a registered nurse who was employed by Baylor Frisco in various capacities from 2002 to November 2011. On or about September 1, 2011, she was promoted from Sr. Vice President, Operations, to Chief Operating Officer ("COO") of Baylor Frisco. On or about August 7, 2002, Ms. Bledsoe signed a Confidentiality and Security Agreement, pursuant to which she agreed as follows:

I understand that Frisco Medical Center (the "Hospital")...must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Hospital, I understand that I may come into possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Hospital's Privacy and Security Policies. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

...

6. I will not make any unauthorized transmissions, inquiries, modifications or purgings of Confidential Information.

Ms. Bledsoe also signed a "Receipt and Acknowledgment of Frisco Medical Center Employee Handbook" (the "Acknowledgment of Employee Handbook"), pursuant to which Ms. Bledsoe represented that she understood she would be provided with confidential information that must not be used outside of the necessary course of business. The Employee Handbook also states, "[n]o one is permitted to remove or make copies of any Baylor Medical Center at Frisco records, reports or documents without prior management approval."

In her various positions with Baylor Frisco, including COO, Ms. Bledsoe had access to non-public, confidential and proprietary information, trade secrets, and patient health care information, subject to the limitations set forth in the Confidentiality and Security Agreement and Acknowledgment of Employee Handbook signed by Ms. Bledsoe, both of which delineated that such access was permitted only for job-related duties or in the necessary course of business and prohibited removal or copying of materials without approval. Ms. Bledsoe understood Baylor Frisco endeavored to protect its confidential information, and that as COO, she had responsibilities to ensure that Baylor Frisco met its responsibilities to safeguard the privacy of patient health information, as well as other confidential information.

Ms. Bledsoe resigned from Baylor Frisco on or about November 1, 2011. Ms. Bledsoe resigned from Baylor Frisco to accept a position with Forest Park. Ms. Bledsoe received a written employment offer from Forest Park on October 21, 2011, after receiving an oral offer on October 18, 2011. She accepted the offer on October 23, 2011. She believed that she might be asked to leave Baylor Frisco upon tendering her resignation.

Michael R. Bledsoe ("Mr. Bledsoe") was employed by Baylor Frisco for approximately nine years, and most recently served as the Information Systems Administrator for Baylor Frisco. On or about August 26, 2002, Mr. Bledsoe signed a Confidentiality and Security Agreement which contained the same definition of "Confidential Information" as the Confidentiality and Security Agreement signed by Ms. Bledsoe.

On June 23, 2006, and on December 16, 2010, Mr. Bledsoe signed acknowledgments that he received Baylor Frisco's Employee Handbook, pursuant to which Mr. Bledsoe agreed that he understood he would be provided with confidential information that must not be used outside of the

necessary course of business. As Information Systems Administrator, Mr. Bledsoe had administrative access to all network systems of Baylor Frisco, and therefore had the ability to access non-public, confidential and proprietary information, and trade secrets, subject to the limitations set forth in the Confidentiality and Security Agreement and Acknowledgments of Employee Handbook signed by Mr. Bledsoe, all of which delineated that such access was permitted only for job-related duties or in the necessary course of business and prohibited removal or copying of materials without approval. On or about December 13, 2011, Mr. Bledsoe tendered a letter of resignation stating that his last day of employment would be December 26, 2011.

After tendering her resignation, Ms. Bledsoe contacted Margaret Garcia, Baylor Frisco's Manager of Human Resources and, in a conversation about her departure, Ms. Bledsoe made a reference that "...she knew where too many bodies were buried." Upon learning about Ms. Bledsoe's comment, Baylor Frisco retained Hewlett-Packard ("HP") IT Security Investigations to conduct a forensic investigation of the computer equipment of Ms. Bledsoe and Mr. Bledsoe (collectively, "Bledsoe Defendants"). HP IT Security Investigations conducted its investigation and issued a report reflecting its findings and conclusions on January 6, 2012 (the "HP Report").

The HP Report provides a detailed description of the investigation, which included an examination of the desktop system assigned to and utilized by Ms. Bledsoe while she was employed with Baylor Frisco, as well as the examination of two laptop computers and an Apple iPad assigned to and utilized by Mr. Bledsoe while he was employed by Baylor Frisco. The investigation also included the examination and analysis of the network user home drives stored on Baylor Frisco servers for both Ms. Bledsoe and Mr. Bledsoe, as well as the Outlook Exchange accounts for both individuals, all of which were offloaded and provided to HP IT Security Investigations for

examination and analysis.

The investigation revealed that both Ms. Bledsoe and Mr. Bledsoe utilized “Dropbox,” a web-based file hosting service that uses “cloud” storage to enable users to store and share files with others across the Internet using file synchronization. When files are uploaded to Dropbox by a user, they automatically “sync” with another computer selected by the user, meaning that the files are transferred from one computer to another.

The investigation revealed that Ms. Bledsoe uploaded numerous folders and/or files containing statutorily protected patient health care information, privileged peer review materials, and highly confidential and proprietary information and trade secrets belonging to Baylor Frisco from her assigned Baylor Frisco computer to her Dropbox account from the period of October 25, 2011, through October 31, 2011.

A review of Ms. Bledsoe’s “Home” drive contained within the Baylor Frisco computer network revealed that the file “Pt info.pdf” was located within the folder/file structure “Dropbox\Medical Staff\Peer Review\PR Letters\PR086.” It appears that Ms. Bledsoe uploaded the file “Pt info.pdf” to Dropbox when she uploaded the folder “Dropbox\Medical Staff\Peer Review\PR Letters.” Sharon Kucyk, the HP forensic analyst who conducted the investigation, concluded that this file and other documents within the folder contained confidential patient information.

Upon review of these folders and/or files, Baylor Frisco determined that they contained protected confidential patient information, peer review materials, confidential and proprietary business information and trade secrets of Baylor Frisco. Baylor Frisco also concluded that the files named “Pt info.pdf” and “SKMBT_C35311103110390.PDF” contain protected health information, including the name of the patient, address, telephone number, and clinical information. The above

folder and files that have “Medical Staff/Peer Review” as part of the folder or file name contain information relating to reviews conducted by the Baylor Frisco peer review committee, which is privileged and confidential. One file includes Baylor Frisco’s strategic business plan data, which is confidential. The above files also included copyrighted material such as the file named “Just Culture Training\Baylor_Frisco - Continuing the Just Culture Journey_Print.ppt.” The information in this file is subject to the terms of “Safe Choices End User License Agreement” between Baylor Frisco and Outcome Engineering, LLC, and Baylor Frisco paid in excess of \$10,000 to obtain this license and has invested substantial additional funds associated with training and implementation of this program.

The HP Report also indicated that Mr. Bledsoe also utilized Dropbox to upload files to his personal Dropbox account. The investigation revealed that Mr. Bledsoe “wiped clean” and reset the Apple iPad assigned to him for use at Baylor Frisco. Mr. Bledsoe also impeded the investigation by modifying permissions that were non-standard to Baylor Frisco’s policies and procedures. For example, Mr. Bledsoe admitted in his deposition to “wiping” the Apple iPad2 clean in order to prevent Baylor Frisco from viewing its contents.

The investigation established that Ms. Bledsoe uploaded Baylor Frisco’s confidential and proprietary information, trade secrets, peer review materials, and statutorily protected patient health information to her personal Dropbox account immediately prior to submitting her resignation with Baylor Frisco. These actions were in direct violation of the terms of her Confidentiality and Security Agreement and the agreements contained in her Acknowledgment of Employee Handbook.

After HP issued its report, Baylor Frisco retained Navigant Consulting (PI) LLC (“Navigant”) to conduct a thorough forensic investigation of the Baylor Frisco-issued computer equipment of

Cindy Bledsoe and Mike Bledsoe. Navigant conducted an investigation and issued a report reflecting its findings and conclusions on March 28, 2014 (the “Initial Navigant Report”). On April 22, 2014, Navigant issued a supplemental report reflecting additional findings and conclusions (the “Supplemental Navigant Report,” together with the Initial Navigant Report, the “Navigant Reports”).

Navigant conducted a forensic investigation of four computer hard drive images owned by Baylor Frisco and formerly assigned to the Bledsoe Defendants, forensic images of two USB thumb drives from Alan Willis, the contents of two network home directories of “shared drives” assigned to Cindy Bledsoe and Mike Bledsoe, and an iPad from Mr. Bledsoe.

Navigant’s investigation of the desktop computer system assigned to and utilized by Ms. Bledsoe revealed that Ms. Bledsoe installed Dropbox on her computer on October 21, 2011, approximately ten days before she resigned from Baylor Frisco and after she had accepted employment with Forest Park. The investigation further revealed that Dropbox was uninstalled from Ms. Bledsoe’s computer on October 31, 2011, one day before she tendered her letter of resignation to Baylor Frisco.

Ms. Bledsoe’s computer was configured to sync her network home folder (the “H” drive residing on Baylor Frisco’s network) with Dropbox, meaning that the files and folders within her network home folder were transferred or uploaded to Dropbox. Navigant’s analysis of the contents of Ms. Bledsoe’s Dropbox folder on her “H:” drive (which were synced to her Dropbox account) revealed folders containing Baylor Frisco’s confidential information and data were transferred to Dropbox by Ms. Bledsoe. Within these folders, Navigant was able to determine that Ms. Bledsoe synced, at a minimum, the following files between her Baylor Frisco computer and her home computer using Dropbox:

H:\Dropbox\Business Planning\2012 Business Planning\Business Plan]2012
 Strategies_Packet.pdf
 H:\Dropbox\cbledsoe.xlsx
 H:\Dropbox\Just Culture Training\A Just Culture.pptm
 H:\Dropbox\Just Culture Training\Baylor_Frisco]Continuing the Just Culture
 Journey_Print.pptx
 H:\Dropbox\Just Culture Training\Creating a Just Culture.ppt
 H:\Dropbox\Just Culture Training\Creating a Just Culture_2010.pptx
 H:\Dropbox\Medical Staff\Peer Review\[redacted]\ [redacted]_Oct 2011 MSPRC.pdf
 H:\Dropbox\Medical Staff\Peer Review\[redacted]\ [redacted]_Oct 31 2011 letter.doc
 H:\Dropbox\Medical Staff\Peer Review\[redacted]\Message from KMBT_C353.msg
 H:\Dropbox\Medical Staff\Peer Review\PR Letters\Herzog Dec 9 2008.doc
 H:\Dropbox\Mom.s folder\3stooges.jpg
 H:\Dropbox\Mom.s folder\Bo05.jpg H:\Dropbox\Mom.s folder\brownie man.JPG
 H:\Dropbox\Mom.s folder\Copy of picture 050.jpg H:\Dropbox\Mom.s folder\Field trip
 014.jpg
 H:\Dropbox\Mom.s folder\Nick 4.JPG H:\Dropbox\Mom.s folder\Nick at the Creek 008.jpg
 H:\Dropbox\Mom.s folder\Nick.s B]Day party 044.jpg
 H:\Dropbox\Mom.s folder\Reed_Navy Man.jpg

Navigant also concluded that Ms. Bledsoe had accessed several files and folders demonstrating knowledge on Ms. Bledsoe's part that such files were in her Dropbox account. Specifically, Exhibit 4 to the Supplemental Navigant Report revealed 358 individual files synced to Ms. Bledsoe's home computer from her Dropbox. Many of these folders and files that Ms. Bledsoe appropriated (notably, numbers 54 through 83 in Exhibit 2 of the Supplemental Navigant Report) contain or consist of documents containing protected health information—including the names of and clinical information relating to patients, privileged and confidential peer review materials, strategic business plans, copyrighted material for which Baylor Frisco paid licensing fees, proprietary program information specifically developed by Baylor Frisco, and sensitive financial information.

For example, the "Sr Leadership" folder contains numerous Monthly Operations Reports ("MORs"), which highlights achievements and opportunities for improvements in various areas such as customer service, technology, community involvement, recruitment/retention, clinical excellence,

quality management, and finance/growth. The MORs also contain confidential and sensitive financial information. The “Sr Leadership” folder also contains documents relating to a Life Safety Action Plan developed by Baylor Frisco, a 2011 Business Action Plan, emails, documents relating to Incentive Planning that divulge information about the financial performance of Baylor Frisco, a document that identifies occurrences at Baylor Frisco and risks associated with those occurrences, a document relating to Baylor Frisco’s planning of a Community Health Fair (which Baylor Frisco developed and implemented over a ten-year period), documents relating to a Resource Utilization Project being developed by Baylor Frisco, documents relating to drug screening of Baylor Frisco employees, a salary grid and compensation information regarding Baylor Frisco employees for which Baylor Frisco paid consultants to develop, and documents relating to exclusive programs and curriculum that Baylor Frisco paid consultant Jon Stigliano to develop and implement. In total, the “Sr Leadership” folder contains over 500 files/documents representing data and information compiled by Baylor Frisco that was only accessible by senior executives.

The “Medical Staff\Peer Review” folder contains hundreds of documents pertaining to Baylor Frisco’s peer review activities, which are confidential and privileged pursuant to state and federal law. Such documents include multiple Medical Staff Reappointment Profiles, which provide information about doctors such as number of patient contacts, clinical performance reviews, and evaluations, and conclude with a recommendation of whether the doctor should be reappointed to his department, and communications with physicians regarding peer review activities.

The “Employee Issues” folder contains over 700 documents, including documents regarding Baylor Frisco’s Employee Performance Improvement Plan, which is a program developed by Baylor Frisco and used to evaluate employees, set expectations for employees, and outline actions to take

to facilitate an employee's success. The "Employee Issues" folder also contains a master list of physicians for peer review purposes, Medical Executive Meeting minutes, as well as highly confidential and sensitive documents regarding resignations, terminations, behavior concerns, and conflicts between employees.

The information and trade secrets contained in the folders and/or files, including but not limited to its business methods and strategies, marketing approach, processes and procedures, and proprietary programs are not known outside of Baylor Frisco, nor are they available to the general public (access to Baylor Frisco's computer network is password-protected). Baylor Frisco takes steps to ensure that this information is and remains confidential and limits access to the above-described information and trade secrets within the facility itself. Baylor Frisco goes to great lengths to protect such confidential and proprietary information and trade secrets, including requiring the limited number of executive-level employees with access to Baylor Frisco's trade secrets to sign Confidentiality and Security Agreements and Acknowledgments of Employee Handbooks, as described above. Further, Baylor Frisco's Information Technology department tailors an employee's access to documents and data available on Baylor Frisco's computer network based upon his or her job description and seniority. Baylor Frisco vigorously protects its confidential and proprietary information and trade secrets because such information and trade secrets are extremely valuable to Baylor Frisco, and equally valuable to its competitors such as Forest Park. Baylor Frisco has expended substantial amounts of time, effort, and money in developing its confidential and proprietary information and trade secrets, which cannot be easily obtained or duplicated by individuals both within and outside of Baylor Frisco due to Baylor Frisco's security measures.

Shortly before uninstalling Dropbox, Ms. Bledsoe also connected two external USB storage

devices to her computer. USB storage devices are a common method to transfer files and folders between computers. Navigant's investigation also revealed that Mr. Bledsoe installed Dropbox on one of his Baylor Frisco computers on August 2, 2011, and that this computer was configured to sync the computer's home folder to Dropbox. Navigant also confirmed that the Apple iPad2 assigned to Mr. Bledsoe contained no retrievable user data, and Navigant determined that a user had run a program to wipe the device clean so as to render unrecoverable any information previously stored.

On July 31, 2012, the Court appointed Dennis Williams ("Mr. Williams"), a partner with Pathway Forensics LLC ("Pathway"), to conduct a forensic investigation of the Bledsoe Defendants' personal computer equipment, electronic storage devices, and smart phones. Mr. Williams and Pathway confirmed many of the findings and conclusions reached by Ms. Kucyk, including that Baylor Frisco data had been transferred to Ms. Bledsoe's Dropbox account. Mr. Williams testified at his deposition that adding or transferring files to a Dropbox account is an intentional action.

Mr. Williams and Pathway conducted an investigation, and Mr. Williams issued his Third Party Forensic Examiner Report on October 16, 2012 (the "Williams Report"). The "Executive Summary" of the Williams Report states:

The examination found files, folders and fragments which are responsive to files and folders listed on the Plaintiff's Second Amended Complaint...A Dropbox folder was created on the Bledsoe desktop computer on November 2, 2011. Dropbox is an application which provides Internet storage of files and allows files to be transferred (synchronized) between computers. On the same day, the Bledsoe desktop computer accessed the Baylor Medical Center Frisco (BMFC) [sic] computer system. Then the Desktop computer accessed www.Dropbox.com, an online data storage website. Shortly thereafter and on the same day, files and folders were deleted from the desktop Dropbox folder. Numerous responsive file fragments were recovered from the unallocated space and file slack on the second hard drive in the Bledsoe desktop computer. These files appear to be associated with BMCF. A report showing the carved responsive files is attached to this report as Exhibit B.

Exhibit B to the Williams Report consists of a fourteen-page spreadsheet identifying the files

associated with Baylor Frisco. With regard to this portion of his report, Mr. Williams testified:

Q: In light of the allegations in the complaint that you reviewed, you felt like these events described in your executive summary were significant, correct?

A. Yes, sir.

Mr. Hamilton: Objection, form.

Q. And it would also be accurate to say that in your experience with the FBI and with white collar crime, you found those events to be suspicious, as well?

A. Yes, sir.

As part of the investigation, Mr. Williams and Pathway conducted “text carving searches,” which involves searching unallocated space for deleted information on a second hard drive associated with the Bledsoe Defendants’ desktop computer. These searches revealed “95 unique files” and 203 “responsive text carve files,” and Mr. Williams concluded that “a large number of these carved files appear to be BMCF files. As stated in the Williams Report, non-privileged responsive files were produced to the parties on September 19, 2012. The documents included a spreadsheet of peer review activity from November 2005, form agendas for meetings of Baylor Frisco’s Medical Executive Committee and Medical Staff Peer Review Committee, a memorandum from Ms. Bledsoe to Mr. Keaton regarding the Medical Staff Peer Review Committee dated December 27, 2010, a document relating to the BMCF Senior Management Incentive Program 2010, and an Orientation Outline for “Surgical Fellow/Resident.”

Mr. Williams and Pathway conducted a search of the “carved files for the file path fragments” in order to produce a list of Dropbox file path fragments, which contained “approximately 728 unique file paths, with over 460 file paths with the base path of ‘/incentive planning/medical staff/peer review’” and “approximately 30 unique paths with the base path of ‘/incentive planning/just culture training/.’” Because the file path for the files included a reference to Dropbox, Mr. Williams concluded the files were transferred to the Bledsoe Defendants’ computer

via Dropbox. Mr. Williams provided a list of the Unallocated Dropbox Path Fragments to the parties, which is also attached to the Williams Report as Exhibit D. The Path Fragments existed on the Bledsoe Defendants' desktop computer (via Dropbox).

The "Conclusion" of the Williams Report states:

An examination of the forensic images provided indicated the usage of the Dropbox application on the Bledsoe devices. On November 2, 2011, at 11:54 AM, the Bledsoe Desktop computer accessed the Dropbox website. A few minutes later, a Dropbox folder was created on the computer and it appears the Dropbox application was installed. Later that day the Bledsoe desktop accessed the BMCF server on several occasions Carving and index searching recovered a large number of files and fragments from Bledsoe desktop computer which appear to be BCMF files.

At his deposition, Mr. Williams testified his investigation confirmed that Ms. Bledsoe transferred data from Baylor Frisco via Dropbox to her personal computer.

Following the issuance of the expert reports described above, Baylor Frisco deposed the Bledsoe Defendants. Ms. Bledsoe testified that beginning October 21, 2011, she transmitted folders and files from her computer drive at Baylor Frisco to the Dropbox application she had installed on her Baylor Frisco computer and that this Dropbox application synced with a folder on her home computer to which she alone had access. This data included, among other items, peer review information, Baylor Frisco's monthly operating reports, employee information, and patient medical records. Ms. Bledsoe further testified that she was aware on approximately November 2–3, 2011, that she had downloaded such files to her home computer from Dropbox. In his deposition, Mr. Bledsoe admitted "wiping" the Apple iPad2 clean so as to prevent Baylor Frisco from viewing its contents after Mr. Keaton requested the password for the device.

Baylor Frisco paid Navigant the total sum of \$120,764.37 for Navigant's forensic investigation. Baylor Frisco paid Pathway Forensics the total sum of \$98,148.72 for Pathway

Forensic's forensic investigation. Baylor Frisco has incurred approximately \$1,193,671.44 for attorneys' fees and expenses retaining the undersigned counsel due to the Defendants' actions.

On January 23, 2012, Plaintiff filed suit against the Bledsoe Defendants in the United States District Court for the Eastern District of Texas in this case, styled Frisco Medical Center, L.L.P. d/b/a Baylor Medical Center at Frisco v. Bledsoe et al., Civil Action No. 4:12-cv-00037 (the "Fraud Lawsuit"). The Fraud Lawsuit was set to be tried before a jury on September 15, 2014, and the parties had submitted their pre-trial disclosures. On August 22, 2014, on the eve of trial, the Bledsoe Defendants filed Suggestions of Bankruptcy. On August 25, 2014, this Court stayed the Fraud Lawsuit pending further order of the Court.

On November 25, 2014, Baylor Frisco initiated an adversary proceeding styled Frisco Medical Center, L.L.P. d/b/a Baylor Medical Center at Frisco v. Bledsoe et al. (In re Bledsoe), Adv. No. 14-04102 (Bankr. E.D. Tex. filed Nov. 25, 2014) (the "Adversary Proceeding") and filed its Original Complaint of Frisco Medical Center, L.L.P. to Determine Dischargeability of a Debt Pursuant to 11 U.S.C. § 523 (the "Adversary Complaint"). In the Adversary Complaint, Baylor Frisco sought to have its claims against Defendants, along with its attorneys' fees, costs, and expenses incurred prosecuting the Fraud Lawsuit and the Adversary Complaint, declared non-dischargeable in the Bankruptcy Case pursuant to 11 U.S.C. §§ 523(a)(4) and (6). On February 9, 2015, U.S. Bankruptcy Judge Brenda T. Rhoades entered a Report and Recommendation, recommending that the District Court *sua sponte* withdraw the reference of the Adversary Proceeding. On March 11, 2015, U.S. District Judge Marcia A. Crone granted the Bankruptcy Court's Report and Recommendation and entered an order withdrawing the Adversary Proceeding to the District Court and transferring the case to this Court.

On May 13, 2015, Baylor Frisco filed its Motion for Status Conference, wherein it asked the Court to consolidate the Fraud Lawsuit and the Adversary Proceeding. The Court held a status conference on June 5, 2015. The Court entered its Order consolidating the Fraud Lawsuit and the Adversary Proceeding on June 11, 2015. The Court also issued an Amended Scheduling Order, which sets the final pretrial conference for December 9, 2015.

On August 10, 2015, Plaintiff filed its motion for summary judgment (Dkt. #190). After no response was filed, the Court gave Defendants until September 17, 2015, to file a response to the motion for summary judgment (Dkt. #200). No response was filed.

LEGAL STANDARD

The purpose of summary judgment is to isolate and dispose of factually unsupported claims or defenses. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986). Summary judgment is proper if the pleadings, the discovery and disclosure materials on file, and any affidavits “[show] that there is no genuine dispute as to any material fact and that the movant is entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a). A dispute about a material fact is genuine “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The trial court must resolve all reasonable doubts in favor of the party opposing the motion for summary judgment. *Casey Enters., Inc. v. Am. Hardware Mut. Ins. Co.*, 655 F.2d 598, 602 (5th Cir. 1981) (citations omitted). The substantive law identifies which facts are material. *Anderson*, 477 U.S. at 248.

The party moving for summary judgment has the burden to show that there is no genuine issue of material fact and that it is entitled to judgment as a matter of law. *Id.* at 247. If the movant bears the burden of proof on a claim or defense on which it is moving for summary judgment, it must

come forward with evidence that establishes “beyond peradventure *all* of the essential elements of the claim or defense.” *Fontenot v. Upjohn Co.*, 780 F.2d 1190, 1194 (5th Cir. 1986). Where the nonmovant bears the burden of proof, the movant may discharge its burden by showing that there is an absence of evidence to support the nonmovant’s case. *Celotex*, 477 U.S. at 325; *Byers v. Dallas Morning News, Inc.*, 209 F.3d 419, 424 (5th Cir. 2000). Once the movant has carried its burden, the nonmovant must “respond to the motion for summary judgment by setting forth particular facts indicating there is a genuine issue for trial.” *Byers*, 209 F.3d at 424 (citing *Anderson*, 477 U.S. at 248-49). The nonmovant must adduce affirmative evidence. *Anderson*, 477 U.S. at 257. No “mere denial of material facts nor...unsworn allegations [nor] arguments and assertions in briefs or legal memoranda” will suffice to carry this burden. *Moayedi v. Compaq Computer Corp.*, 98 F. App’x 335, 338 (5th Cir. 2004). Rather, the Court requires “significant probative evidence” from the nonmovant in order to dismiss a request for summary judgment supported appropriately by the movant. *United States v. Lawrence*, 276 F.3d 193, 197 (5th Cir. 2001). The Court must consider all of the evidence, but must refrain from making any credibility determinations or weighing the evidence. *See Turner v. Baylor Richardson Med. Ctr.*, 476 F.3d 337, 343 (5th Cir. 2007).

DISCUSSION AND ANALYSIS

The Court must determine whether the summary judgment evidence cited herein establishes the elements of the four causes of action asserted by Baylor Frisco in the Fraud Lawsuit and whether the Bledsoe Defendants’ liabilities to Baylor Frisco are non-dischargeable as asserted in the Adversary Proceeding.

Claims Under the Computer Fraud and Abuse Act

Baylor Medical asserts that its is entitled to summary judgment on its claims under the

Computer Fraud and Abuse Act (“CFAA”). Under section 1030(g) of the CFAA, “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action” for compensatory damages and injunctive or other equitable relief. 18 U.S.C. § 1030(g). Violations of the CFAA include: (1) intentionally accessing a protected computer without authorization or by exceeding authorization and obtaining information from that computer; (2) knowingly (and with an intent to defraud) accessing a protected computer without authorization or by exceeding authorization and obtaining anything in excess of \$5,000 in value; and (3) intentionally accessing a protected computer without authorization and causing damage and loss. 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), 1030(5)(C). Based upon the summary judgment evidence, Baylor Frisco has established all three violations.

To bring a claim under the CFAA, Plaintiff is required to show damage or loss, but not both. *See* 18 U.S.C. § 1030(g). “Loss” is defined under the CFAA as “any reasonable cost to [the] victim, including the cost of responding to an offense, conducting a damage assessment . . .” and courts have held that the costs of a forensic investigation/damage assessment constitute loss under the CFAA. 18 U.S.C. § 1030(e)(11); *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645–46 (4th Cir. 2009); *See Quantlab Techs. Ltd. (BVI) v. Godlevsky*, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010).

In this case, Baylor Frisco paid Navigant the total sum of \$120,764.37 for Navigant’s forensic investigation, and paid Pathway Forensics the total sum of \$98,148.72 for its forensic investigation, and thus, has demonstrated loss under the CFAA.

Baylor Frisco has established that the Bledsoe Defendants violated section 1030(a)(2)(C) of the CFAA by intentionally accessing a protected computer by exceeding their authorization and obtaining information, which caused loss to Baylor Frisco. First, the Bledsoe Defendants’ access of

Baylor Frisco's computer devices was intentional: Navigant concluded the Bledsoe Defendants' actions were intentional; Mr. Williams testified that transferring files to Dropbox (as performed by Ms. Bledsoe) is a necessarily intentional action; and Mr. Bledsoe testified that he wiped his Baylor Frisco-issued Apple iPad after his wife's resignation. Second, the desktop computer issued to Ms. Bledsoe and the Apple iPad issued to Mr. Bledsoe are protected computers under the definitions set forth in the CFAA.

Next, the Bledsoe Defendants exceeded their authorization in obtaining information from Baylor Frisco's computers. As set forth above, the Bledsoe Defendants signed Confidentiality and Security Agreements pursuant to which they agreed to "access" Baylor Frisco's "Confidential Information" only when necessary to perform job-related duties, and also agreed not to make "unauthorized transmissions" of Confidential Information. In their respective Acknowledgments of Employee Handbooks, the Bledsoe Defendants acknowledged and agreed that "[n]o one is permitted to remove or make copies...of any records, reports or documents without prior management approval." The Bledsoe Defendants did not have management approval to transmit thousands of Baylor Frisco files containing highly confidential and proprietary information, trade secrets, and protected patient information to Dropbox, and ultimately to their personal desktop computer, in the final days of their employment with Baylor Frisco.

The summary judgment evidence in this matter shows the Bledsoe Defendants' accessing, copying and transferring of Baylor Frisco's files constituted access in excess of their authorization. It is undisputed that the Bledsoe Defendants' actions in this regard were not related to their duties as Baylor Frisco employees. The summary judgment evidence establishes the Bledsoe Defendants did not have the authorization to access, copy, and transmit Baylor Frisco files, and that they

exceeded their authorization in doing so. The Bledsoe Defendants obtained information from Baylor Frisco's computers. Specifically, as set forth above in detail, Navigant and Pathway Forensics determined that a significant number of Baylor Frisco files and folders were transferred to Dropbox, and then resided on the Bledsoe Defendants' home computer.

Baylor Frisco has demonstrated loss as defined under the CFAA, and as construed in relevant case law: "the term 'loss' encompasses only two types of harm: costs to investigate and respond to a computer intrusion, and costs associated with a service interruption." Specifically, Baylor Frisco has incurred in excess of \$218,000 in fees paid to forensic experts to uncover the breadth of the Bledsoe Defendants' unauthorized transfers. The summary judgment evidence establishes that the Bledsoe Defendants violated section 1030(a)(2) of the CFAA by intentionally accessing a protected computer by exceeding their authorization and obtaining information, which caused loss to Baylor Frisco.

Baylor Frisco has also established that the Bledsoe Defendants violated section 1030(a)(4) of the CFAA by knowingly accessing a protected computer without authorization or by exceeding authorization and obtaining anything in excess of \$5,000 in value. First, as set forth above, the Bledsoe Defendants' access of protected computers was knowing and intentional. The summary judgment evidence shows that, after accepting a new job, and in the final hours of her employment, Ms. Bledsoe accessed her protected computer and transferred to Dropbox a significant amount of data belonging to Baylor Frisco, and then to the home computer she shared with Mr. Bledsoe—who himself had wiped his Apple iPad in order to prevent the CEO of Baylor Frisco from viewing its content—before making a threatening comment to the Human Resources Manager of Baylor Frisco. The Bledsoe Defendants also exceeded their authorizations to access Baylor Frisco computers.

Finally, the Bledsoe Defendants obtained items with a value exceeding \$5,000. “[T]he typical item of value in CFAA cases is usually data.” *In re Am. Online, Inc.*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001) Identifying the misappropriated data or information is sufficient to show that a defendant obtained valuable information under the CFAA. *Genesco Sports Enter., Inc. v. White*, No. 3:11-CV-1345-N (BF), 2011 WL 6593415, at *6 (N.D. Tex. Oct. 27, 2011). Baylor Frisco identified a significant amount of data misappropriated by the Bledsoe Defendants.

Baylor Frisco has also established a violation of CFAA section 1030(a)(5)(C). To establish a violation of section 1030(a)(5)(C), Baylor Frisco must establish the Bledsoe Defendants intentionally accessed a protected computer without authorization and caused damage and loss. The summary judgment evidence demonstrates the Bledsoe Defendants intentionally accessed protected computers without authorization, causing loss to Baylor Frisco. With regard to section 1030(a)(5)(C)’s requirement that the Bledsoe Defendants’ access cause “damage,” damage includes “any impairment to the integrity . . . of data . . . or information.” *Shurgard Storage Ctr. Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1122 (N.D. Wash 2000) (quoting 18 U.S.C. § 1030(e)(8)(A)). A plaintiff states a valid claim under section 1030(a)(5)(C) even when no data was physically changed or erased, because when the data is misappropriated, an impairment of its integrity occurs. *Id.* at 1127. It is undisputed that Mr. Bledsoe physically erased the existing data on his Apple iPad and that Ms. Bledsoe misappropriated a significant amount of data from Baylor Frisco, thereby impairing its integrity pursuant to *Shurgard*. Therefore, Baylor Frisco has demonstrated that the Bledsoe Defendants caused damage to Baylor Frisco.

Claim for Violation of the Electronic Communications Privacy Act/Stored Communications Act

In order to prevail upon its claim for a violation of the Electronic Communications Privacy Act/Stored Communications Act (“ECPA”), Baylor Frisco must show the Bledsoe Defendants exceeded their authorization to access a facility through which an electronic communication service is provided and obtained an electronic communication while it was in electronic storage. 18 U.S.C. § 2701. The summary judgment evidence demonstrates that Baylor Frisco restricted the Bledsoe Defendants’ access to Baylor Frisco’s computer network, and also prohibited the unauthorized transmission of Baylor Frisco’s “Confidential information.” The Bledsoe Defendants had access to Baylor Frisco’s computer network for business purposes, but not for purposes of transferring sensitive data to themselves. The summary judgment evidence demonstrates that the Bledsoe Defendants far exceeded their authorization to access Baylor Frisco’s computer network, through which electronic communications services are provided. It is also undisputed that in the final days of their employment, the Bledsoe Defendants obtained and transmitted numerous files, while they were in electronic storage at Baylor Frisco, to Dropbox.

Because Baylor Frisco has established a violation of the ECPA, it is entitled to damages and its attorneys’ fees pursuant to 18 U.S.C. § 2707(c). Baylor Frisco’s damages include the sums paid to forensic investigators. From January 1, 2012, through July 31, 2015, Baylor Frisco has incurred \$1,193,671.44 in attorneys’ fees and expenses.

Breach of Contract Claim

Under Texas law, a breach of contract is the failure to perform any promise which forms a whole or part of any agreement. *See DeSantis v. Wackenhut Corp.*, 732 S.W.2d 29, 34 (Tex.

App.—Houston [14th Dist.] 1987), *aff'd in part, rev'd in part on other grounds*, 793 S.W.2d 670 (Tex. 1990). To prevail on a breach of contract claim, a plaintiff must show there is an enforceable contract that was breached by the defendant, which caused the plaintiff injury. *Foley v. Daniel*, 346 S.W.3d 687, 690 (Tex. App.—El Paso 2009, no pet.). The Bledsoe Defendants signed Confidentiality and Security Agreements and Acknowledgments of Employee Handbooks pursuant to which they agreed to use Baylor Frisco's "Confidential Information" solely for job-related functions, and further agreed not to make unauthorized transmissions of such information nor to remove copies of Baylor Frisco's documents without management approval. The Confidentiality and Security Agreements and Acknowledgments of Employee Handbooks not only proscribe the use of Baylor Frisco's Confidential Information, but also prohibit the unauthorized transfer or purging of such information. It is undisputed that Ms. Bledsoe accessed and transferred Baylor Frisco files to Dropbox, and then to the Bledsoe Defendants' home computer, without authorization or management approval, in violation of her agreements with Baylor Frisco. It is also undisputed that Mr. Bledsoe purged the content of his Apple iPad, without authorization or prior approval.

Baylor Frisco has presented summary judgment evidence establishing valid agreements, the breach, and injury resulting from the breach. Therefore, it is entitled to summary judgment on its breach of contract claim. Baylor Frisco is also entitled to recover its attorneys' fees. From January 1, 2012, through July 31, 2015, Plaintiff has incurred \$1,142,979.00 in attorneys' fees.

Considering the time required by the attorneys to properly handle this case, the novelty and difficulty of the questions involved, the skill required to perform the legal services necessary to prosecute and defend the various parties' positions, the fees customarily charged in Collin County, the amount in controversy, and the experience, reputation, and ability of the lawyers performing the

services, the above attorneys' fees and expenses generated and incurred to date are reasonable, and necessary for the work performed in this case. The amount of fees and expenses incurred by Baylor Frisco to date in connection with this litigation is customary for attorneys' fees and expenses charged for similar legal services in Collin County, Texas.

Breach of Fiduciary Duty Claim

In order to prevail upon a claim for breach of fiduciary duty (1) there must be a fiduciary relationship, (2) the defendant must have breached his or her fiduciary duty to the plaintiff, and (3) the breach must cause injury to the plaintiff or benefit to the defendant. *Graham Mortg. Corp. v. Hall*, 307 S.W.3d 472, 479 (Tex. App.—Dallas 2010, no pet.). Under Texas law, it is well-established that general fiduciary duties include the duty of loyalty and good faith, the duty to refrain from self-dealing and the duty to act with integrity. *Hawthorne v. Guenther*, 917 S.W.2d 924, 934 (Tex. App.—Beaumont 1996, writ denied); *Dearing, Inc. v. Spiller*, 824 S.W.2d 728, 732-33 (Tex. App.—Fort Worth 1992, writ denied); *Hartford Cas. Ins. Co. v. Walker Cty. Agency, Inc.*, 808 S.W.2d 681, 687-88 (Tex. App.—Corpus Christi 1991, no writ). Employees such as the Bledsoe Defendants owe a fiduciary duty to their employers and are obligated to act in their employers' interests. *Johnson v. Brewer & Pritchard, P.C.*, 73 S.W.3d 193, 201–02 (Tex. 2002). The Bledsoe Defendants owed Baylor Frisco a fiduciary duty.

The summary evidence shows that the Bledsoe Defendants breached their fiduciary duties to Baylor Frisco by transmitting and misappropriating thousands of highly confidential and sensitive files pertaining to peer review activities, business strategies, employee counseling and supervision, and proprietary programs developed by Baylor Frisco to Dropbox and ultimately to their personal desktop computer, in the final hours of their employment, with the mentality that they knew where

“too many bodies were buried.” Mr. Bledsoe’s intentional deletion of the data on Baylor Frisco’s Apple iPad also constituted a breach of his fiduciary duties. Finally, Baylor Frisco has been injured as a result of the Bledsoe Defendants’ breach of their fiduciary duties, having incurred over \$218,000 in forensic investigation costs. Baylor Frisco has established its breach of fiduciary duty claims against the Bledsoe Defendants, and it is entitled to summary judgment.

Debts Are Not Dischargeable in Bankruptcy

Section 523(a)(4) of the Bankruptcy Code excepts from discharge an individual debtor’s debts “for fraud or defalcation while acting in a fiduciary capacity, embezzlement, or larceny.” 11 U.S.C. § 523(a)(4). While the scope of the fiduciary capacity under section 523(a)(4) is a question of federal law, the Fifth Circuit has noted that “state law is important in determining whether or not a trust obligation exists.” *LSP Inv. P’ship v. Bennett (In re Bennett)*, 989 F.2d 779, 784 (5th Cir. 1993).

The Fifth Circuit has “not hesitated to conclude that debts arising from misappropriation by persons serving in a traditional, pre-existing fiduciary capacity, as understood by state law principles, are non-dischargeable.” *Gupta v. E. Idaho Tumor Institute, Inc. (In re Gupta)*, 394 F.3d 347, 350 (5th Cir. 2004). A debt may be non-dischargeable under section 523(a)(4) even absent a fiduciary relationship if the debtor commits embezzlement or larceny. 11 U.S.C. § 523(a)(4); *Miller v. J.D. Abrams Inc. (In re Miller)*, 156 F.3d 598, 602 (5th Cir. 1998). Embezzlement for the purposes of section 523(a)(4) is “the fraudulent appropriation of property by a person to whom such property has been entrusted, or into whose hands it has lawfully come.” *Moraine v. Nazarko (In re Nazarko)*, Adv. No. 05–4270, 2008 WL 304785, at *5 (Bankr. E.D. Tex. Jan. 31, 2008) (citing *Miller*, 156 F.3d at 602).

Baylor Frisco has demonstrated that the Bledsoe Defendants owed and breached fiduciary duties to Baylor Frisco by misappropriating Baylor Frisco's data, and in the case of Mr. Bledsoe, destroying data on a device belonging to Baylor Frisco, in the final days of their employment with Baylor Frisco. Baylor Frisco has also demonstrated that the Bledsoe Defendants committed embezzlement as defined under section 523(a)(4). The summary judgment evidence conclusively establishes that the Bledsoe Defendants' debts under the Fraud Lawsuit are non-dischargeable pursuant to section 523(a)(4) of the Bankruptcy Code.

Baylor Frisco also asserts that section 523(a)(6) bars discharge of the Bledsoe Defendants' indebtedness because they willfully and maliciously injured Baylor Frisco and its property. Section 523(a)(6) of the Code excepts from discharge any debts incurred by "willful and malicious injury by the debtor to another entity or to the property of another entity." 11 U.S.C. § 523(a)(6); *Kawaauhua v. Geiger*, 523 U.S. 57, 61 (1998). The Fifth Circuit uses an implied malice standard for section 523(a)(6) such that a debtor causes willful and malicious injury where there is either: (1) an objective substantial certainty of harm arising from a deliberate or intentional action or (2) a subjective motive to cause harm by a party taking a deliberate or intentional action. *Miller*, 156 F.3d at 605-606. An intentional breach of contract claim, where accompanied by malicious and willful tortious conduct, will satisfy the requirements of section 523(a)(6). *Eagles Sindh, Inc. v. Desai (In re Desai)*, Adv. No. 07-04190, 2009 WL 2855735, at *6 (Bankr. E.D. Tex. Sept. 2, 2009).

Baylor Frisco has established that the Bledsoe Defendants breached their respective agreements with Baylor Frisco, and that their actions were intentional. The Bledsoe Defendants also violated federal law in accessing, and then transmitting, data and email without authorization. The Bledsoe Defendants' conduct, which Baylor Frisco has shown to be deliberate, satisfies both prongs

of the Fifth Circuit's implied malice standard.

Baylor Frisco has sought attorneys' fees, expenses, and costs in the Fraud Lawsuit pursuant to 18 U.S.C. § 2707(c), Texas Civil Practice & Remedies Code § 38.001 *et seq.*, and as otherwise permitted by law. Attorneys' fees, expenses, and costs awarded as part of a judgment establishing a debtor's fraud are not dischargeable through bankruptcy. *Cohen v. de la Cruz*, 523 U.S. 213, 223 (1998). Reasonable attorneys' fees, expenses, and costs incurred in connection with adversary proceedings to declare non-dischargeable debts incurred by a debtor's fraud are also excepted from discharge. *Id.* Therefore, Plaintiff is entitled to recover reasonable attorneys' fees, expenses, and costs in prosecuting the Adversary Proceeding and to have those amounts be excepted from discharge in the Bledsoe Defendants' Chapter 7 bankruptcy case.

CONCLUSION

It is therefore **ORDERED** that Plaintiff's Motion for Summary Judgment (Dkt. #190) is hereby **GRANTED**. Plaintiff is instructed to submit to the Court a proposed Final Judgment within seven (7) days of entry of this Memorandum Opinion.

SIGNED this 30th day of November, 2015.


AMOS L. MAZZANT
UNITED STATES DISTRICT JUDGE